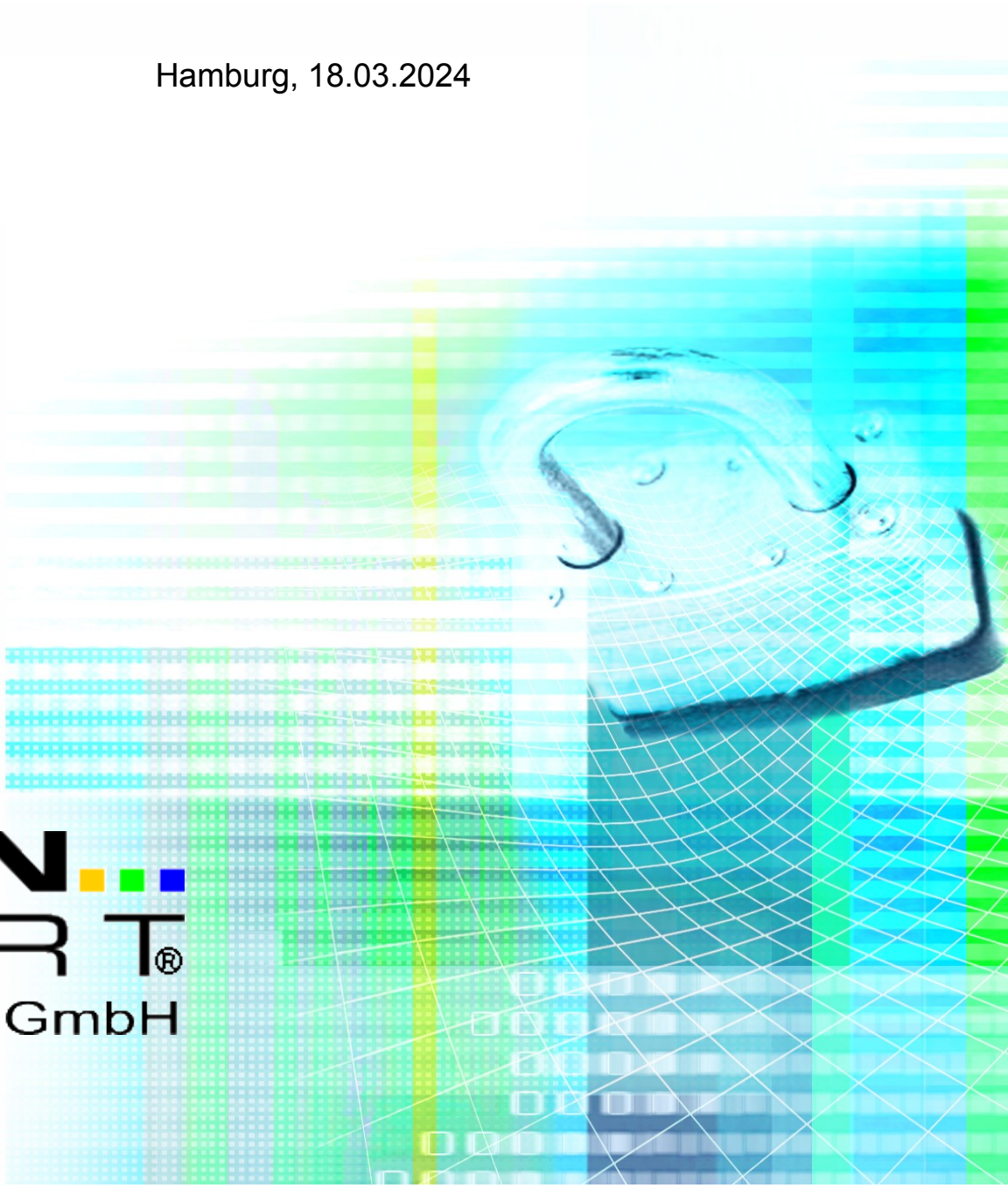
DNS-RPZ

- Teil 1: Grundlegende Informationen -

Hamburg, 18.03.2024



DFN-CERT® Services GmbH

Dokument-Informationen	
Sperrvermerk	Nur für: DFN-CERT Services GmbH, DFN-Verein, Teilnehmer und Interessierte am Dienst DFN.Security
Dateiname	DNS-RPZ_Grundlegende_Informationen.odt
letzte Bearbeitung	Montag, 18. März 2024
Seitenanzahl	11
URL aktuelle Version	https://www.dfn-cert.de/leistungen/security-operations/

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einführung

1.1 Ziel dieses Dokuments

Dieses Dokument dient dazu, einen Überblick über die Funktionsweise von DNS-RPZ (Domain Name System Response Policy Zones) und der Teilnahme am Leistungsmerkmal DNS-RPZ im Rahmen des Dienstes DFN.Security zu schaffen.

1.2 Zielgruppe dieses Dokuments

Dieses Dokument ist adressiert an alle Personen, die an der Teilnahme an dem Leistungsmerkmal DNS-RPZ im Dienst DFN.Security interessiert sind.

1.3 Grenzen dieses Dokuments

Die Erfassung von Teilnehmerdaten für die Inbetriebnahme von DNS-RPZ ist in das Dokument DNS-RPZ_Teilnehmerdaten.pdf ausgelagert. Das Formular liefert die Informationen, die das DFN-CERT braucht, um die Konfiguration für die Dienstanbindung der teilnehmenden Organisation vorzunehmen.

Das Dokument DNS-RPZ_Administration.pdf dient als Hilfestellung, um DNS-RPZ mit der DNS-Software BIND zu konfigurieren.

Alle Teile der Dokumentation sind unter https://www.dfn-cert.de/leistungen/security-operations/ im Abschnitt DNS-RPZ zu finden.

2. Aufbau und Funktionsweise von DNS-RPZ

DNS-RPZ (Domain Name System Response Policy Zone) ist ein Verfahren (siehe Abbildung 1), um bei der Namensauflösung durch rekursive DNS-Resolver mittels eigener Richtlinien einzugreifen und dadurch letztlich den Zugriff auf bestimmte Domains zu unterbinden. DNS-RPZ wurde ursprünglich vom einem Team des Internet System Consortium (ISC) unter der Leitung von Paul Vixie entwickelt und als Internet Engineering Task Force (IETF)-Entwurf im Jahr 2010 veröffentlicht. Im selben Jahr wurde die erste funktionsfähige DNS-RPZ-Erweiterung für die DNS-Software BIND im Zusammenhang mit diesem Entwurf bereitgestellt. Grundsätzlich ist es aber ein offenes und herstellerunabhängiges Verfahren. Die letzte Version von dem Entwurf ist zu finden unter https://datatracker.ietf.org/doc/html/draft-vixie-dnsop-dns-rpz und trotz des Ablaufdatums (23.12.2018) nach wie vor aktuell.

Stellen Nutzer eine DNS-Anfrage für eine Seite mit maliziösen Inhalten (Schritt 1), die in einer eingebundenen Zone (Schritt 0) gelistet ist, liefert der DNS-Server nicht die IP-Adresse des eigentlich angefragten bösartigen Ziels, sondern die einer sogenannten Landingpage (Schritt 2) zurück. Statt auf eine Seite mit maliziösen Inhalten greifen Nutzer – sofern sie bei ihrer Anfrage auf den Einsatz von TLS (Transport Layer Security) verzichten oder die üblicherweise angezeigte Zertifikatswarnung akzeptieren – auf eine sichere Landingpage (Schritt 3) zu, die sie darüber informiert, dass das gewünschte Ziel als bösartig eingestuft ist und ihre Anfrage daher umgeleitet wurde.

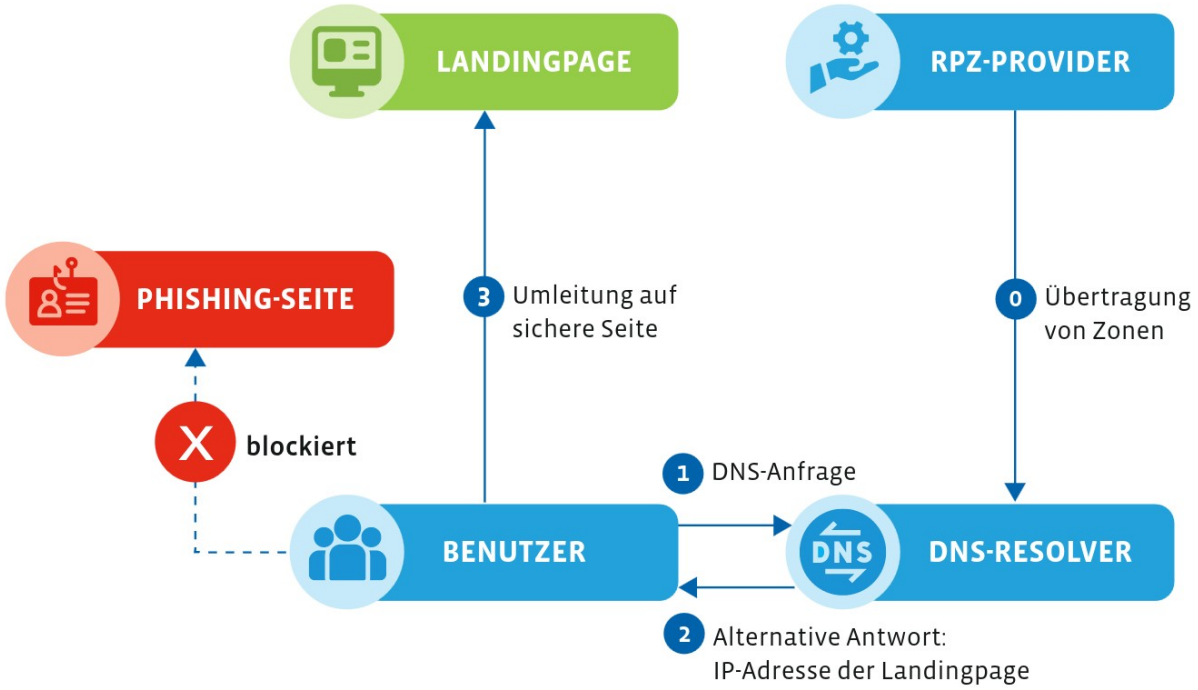


Abbildung 1: Schematische Darstellung von DNS-RPZ

Die Funktionsweise ist hier anhand von Web-Zugriffen über HTTP bzw. HTTPS veranschaulicht, grundsätzlich ist DNS-RPZ aber protokollunabhängig und kann für jeglichen Datenverkehr genutzt werden, solange DNS für die Namensauflösung eingesetzt wird.

Konkret wird über den Dienst DFN.Security ein Feed (genauer: mehrere Response Policy Zonen) bereitgestellt, in dem Informationen zu maliziösen Domains gesammelt zur Verfügung stehen. Wird eine Zone aufgrund neuer Erkenntnisse aktualisiert, wird der DNS-Server des Teilnehmers über einen sogenannten Notify informiert. Durch den automatischen Abruf der aktualisierten Zone, den sogenannten Zonentransfer, und die Einbindung in das eigene DNS wird direkt auf neu ermittelte Bedrohungen reagiert – so werden Nutzer bereits vor dem Besuch einer bösartigen Webseite geschützt.

Die sichere Landingpage kann von der teilnehmenden Einrichtung selbst bereitgestellt werden. Alternativ kann das mit den Einrichtungsinformationen angereicherte Template des Dienstes DFN.Security eingesetzt werden. In jedem Fall sollte die Landingpage über den Vorgang, den Grund für die Blockierung sowie die zur Verfügung stehende Handlungsmöglichkeit informieren.

Die Schweizer Stiftung SWITCH betreibt seit Jahren unter dem Namen DNS-Firewall u.a. für die Schweizer Hochschulen einen DNS-RPZ-Dienst. Die Ähnlichkeit des Einsatzgebiets wie auch die bisher vom DFN-CERT durchgeführten Tests sprechen dafür, dass die von SWITCH erstellten Response Policy Zonen auch für Teilnehmer am Deutschen Forschungsnetz eine hohe Relevanz haben. Um den DFN-Teilnehmern das neue Dienstmerkmal DNS-RPZ zügig bereitzustellen und einen optimalen Austausch vertraulicher Informationen zwischen dem DFN-Verein und SWITCH zu gewährleisten, ist eine Übereinkunft für eine Forschungskooperation getroffen worden. In diesem Kontext muss unbedingt auch die Dienstbeschreibung beachtet werden, insbesondere, dass das Extrahieren von Daten aus dem DNS-RPZ-Feed und deren Verwendung in anderen Systemen, wie SIEMs, Web Application Firewalls usw., untersagt ist. Dies ist eine Anforderung, die wir von SWITCH weitergeben müssen.

Im Rahmen der Zusammenarbeit stellt SWITCH dem DFN-Verein in einem ersten Schritt seine Technik und Expertise zu DNS-RPZ zur Verfügung. Das umfasst die Beratung beim Systemdesign sowie die Freigabe der Nutzung der SWITCH-Zonen für alle Teilnehmer am Dienst DFN.Security. Der zweite Schritt richtet sich auf den Austausch von Daten zur Verbesserung der Zonen und die voraussichtliche Erstellung weiterer Zonen, die sowohl für Nutzer des SWITCH-Dienstes als auch für DFN-Teilnehmer verfügbar sind. Ziel ist es, allen Einrichtungen im Deutschen Forschungsnetz umfassende Angebote zur Informationssicherheit bereitzustellen, die in der Praxis von möglichst vielen Teilnehmern genutzt werden. Denn Netzwerksicherheit bedarf der Anstrengung aller in der Hochschul- und Forschungsgemeinschaft.

Es ist trotz aller Sorgfalt beim Erstellen der Zonen möglich, dass eine Domain fälschlicherweise blockiert wird. In diesem Fall können Nutzer das Entfernen der Domain aus der Liste der maliziösen Domain beantragen. Als schnelle Antwort auf eine Anforderung zum Entblocken kann eine Einrichtung die betreffende Domain selbst in eine eigene Ausnahmeliste (White-List) auf dem DNS-Server eintragen und dadurch den Zugriff für die eigenen Nutzer kurzfristig wieder freigeben. Zusätzlich sollte die Information über das ungerechtfertigte Blocken – ein sogenannter „false positive“-Eintrag – an den Feed-Provider

weitergeleitet werden, damit dieser die Domain aus der RPZ entfernt und somit den Zugriff für alle Teilnehmer an diesem Dienstmerkmal wieder freigibt.

Teilnehmer, die DNS-RPZ einsetzen wollen, haben durch die im Dienst DFN.Security enthaltene Logdatenanalyse die Möglichkeit, sich einen Überblick über die Vorgänge in der eigenen Einrichtung zu verschaffen. Mit dem Übermitteln der betreffenden DNS-Server-Logs werden die geblockten Zugriffsversuche in Form automatischer Warnmeldungen für Administratoren zusammengefasst.

3. Einrichtung und Betrieb von DNS-RPZ

Die Einrichtung von DNS-RPZ umfasst einige wenige Schritte der teilnehmenden Organisation, die im Folgenden ausgeführt werden.

3.1 Konfiguration des DNS-Servers auf der Seite der teilnehmenden Organisation

Das Dokument DNS-RPZ_Administration.pdf dient als Hilfestellung, um DNS-RPZ mit der DNS-Software BIND im Rahmen des Dienstes DFN.Security zu konfigurieren.

3.1.1 DNS-Server mit RPZ-Support

Neben der Teilnahme an Dienst DFN.Security erfordert die Nutzung dieses Angebots den Betrieb eines DNS-Servers, der RPZ unterstützt. Als DNS-Software stehen derzeit BIND, PowerDNS Recursor oder Knot Resolver zur Verfügung. Alternativ ist der Einsatz einer DNS-Appliance wie Infoblox, BlueCat, EfficientIP oder Nokia VitalQIB (Quelle: SWITCH) möglich.

3.1.2 Zonen

Zonen dienen im DNS dazu, für bestimmte (Sub-)Domains die Namensauflösung durchzuführen. Diese Struktur kann auch genutzt werden, um Zugriffe auf bekannte, bösartige Domains auf eine vorher definierte, sichere Landingpage umzuleiten. Response Policy Zonen werden dazu vor allen anderen Zonen eingesetzt, sodass zuerst gefiltert wird und die Anfrage erst danach wie üblich weiter abgearbeitet wird.

Eine genaue Aufschlüsselung der Zonen vom DFN-CERT und SWITCH mit ihren Aufgaben können ist im vorgenannten Dokument vorhanden. Eine besondere Zone ist die Community-Zone, die für zukünftige Inhalte vorbereitet ist und erst zu einem späteren Zeitpunkt definiert wird. In der aktuell vorliegenden Konfiguration wird sie daher rein passiv eingesetzt.

3.1.3 Einrichten einer eigenen Landingpage

Die teilnehmenden Organisationen können eine vom DFN-CERT bereitgestellte standardisierte Web-Seite als Landingpage für blockierte Web-Zugriffe nutzen (zu sehen unter https://landingpage-ph.security.dfn.de) oder eine eigene verwenden. In letzterem Fall ist zusätzlich das Aufsetzen eines HTTP(S)-Servers mit einer entsprechenden Web-Seite notwendig, zu der die Benutzer umgeleitet werden können. Es ist dabei zu beachten, dass durch die protokollunabhängige Funktionsweise von DNS-RPZ auch blockierte Zugriffe anderer Protokolle auf dieser Server-Adresse auf deren spezifischen Ports ankommen und nicht auf den HTTP(S)-Ports. Die Landingpage hilft in den Fällen also nicht weiter.

3.1.4 Lokale Ausnahmeliste und Meldung von Fehlern

Es kann bei „false positives“ kurzfristig notwendig oder zu Forschungszwecken sinnvoll sein, blockierte Domains zugänglich zu machen, ohne dass sie vom DFN-CERT kontrolliert und verifiziert werden müssen. Dafür ist eine lokale Ausnahmeliste erforderlich, die durch die teilnehmende Organisation eigenständig einzurichten ist. Hinweise dazu finden sich im oben genannten Dokument.

Sollten Domains fälschlicherweise geblockt sein, dann ist eine Kontaktaufnahme mit den Ansprechpartnern des DFN-CERTs (siehe Kapitel 3.5) wünschenswert, damit auch die anderen teilnehmenden Organisationen von der Fehlerbehebung profitieren können.

3.2 Konfiguration auf der Seite des DFN-CERTs

Das DFN-CERT benötigt bestimmte Informationen, um die Konfiguration für die Dienstanbindung der teilnehmenden Organisation vornehmen zu können. Diese müssen in die Formularfelder in dem Dokument DNS-RPZ_Teilnehmerdaten.pdf eingetragen werden. Das Formular ist vollständig ausgefüllt zu senden an die Adresse des DFN-CERTs (siehe Kapitel 3.5).

Eine dieser Informationen ist der Name der Organisation wie er im DFN.Security-Portal angegeben ist. Aus dem Portal können anhand dieser ID bereits einige Informationen entnommen werden, so dass sie nicht noch einmal im Formular angegeben werden müssen.

Dazu zählen u.a. die verifizierten Domains der Organisation. Das DFN-CERT unterhält eine Ausnahmeliste mit Domains, welche grundsätzlich nicht geblockt werden sollen. Aus den verifizierten Domains aller Organisationen wird dazu eine kombinierte Ausnahmeliste als eigene Zone des DFN-CERTs erstellt.

Des weiteren werden die Netzbereiche der Organisation für die Zuordnung der von ihnen ausgehenden Client-Zugriffe zu der vom DFN-CERT bereitgestellten Landingpage benötigt. In das Template dieser Landingpage wird ein im Formular anzugebender Helpdesk-Kontakt der Organisation eingebettet, an den sich die Benutzer der Organisation mit Fragen oder Problemen wenden können. Aufgrund der Herkunftsbestimmung der Client-Zugriffe auf diese Landingpage wird die Auswahl des passenden Helpdesk-Kontakts vorgenommen.

Damit die Daten des DNS-RPZ-Feeds mittels Zonentransfer an die Organisation übertragen werden können, ist die Angabe der IP-Adressen der DNS-Server zwingend erforderlich.

Es ist für den zukünftigen Betrieb wichtig, dass all diese Daten von den teilnehmenden Organisationen unbedingt stets aktuell gehalten werden müssen!

3.3 Logdatenanalyse

Die Konfiguration der bereitgestellten Zonen ist so eingestellt, dass geblockte DNS-Anfragen durch DNS-RPZ protokolliert werden. Die Log-Daten bieten einen Einblick in

möglicherweise sicherheitsrelevante Vorfälle, da durch Angreifer bereitgestellte URLs und Schadsoftware, die es ins lokale Netz geschafft hat, häufig einen Kontakt zu maliziösen Domains aufnehmen, um Informationen preiszugeben, ungewollte Aktionen auszulösen, Software nachzuladen oder von diesen Befehle entgegen zu nehmen. Eine Analyse des Loggings kann also Aufschluss über Angriffe und kompromittierte Systeme zu geben.

Für eine automatische Analyse der Logdaten ist das SOC (Security Operations Center)-System als Bestandteil des Dienstes DFN.Security vorgesehen. Die Anbindung an die Logdatenanalyse und weitere Informationen sind unter https://www.dfn-cert.de/leistungen/security-operations/ zu finden.

3.4 Mailingliste für DNS-RPZ-Teilnehmer

Für den gegenseitigen Austausch der Teilnehmer untereinander gibt es die Möglichkeit, sich bei der öffentlichen Mailingliste dfnsecurity-dns-rpz@listserv.dfn.de anzumelden. Die angemeldete Adresse wird dann durch die Administration freigeschaltet und darüber benachrichtigt.

3.5 Ansprechpartner beim DFN und DFN-CERT

Sowohl die Logdatenanalyse als auch die Nutzung von DNS-RPZ erfordert, dass mindestens die Dienstvereinbarung für die DFN.Security Basisleistungen unterzeichnet wurde. Ein Zugang zu den Systemen kann sonst nicht eingerichtet werden. Ansprechpartner ist der DFN über die Adresse dfn.security@dfn.de.

Bei technischen Problemen, Feedback, Fragen und Anregungen können Ansprechpartner beim DFN-CERT via dns-rpz@dfn-cert.de weiterhelfen.

